Tomorrow's Affairs
Analysis of today
Assessment of tomorrow

By: Sally Wentworth

A digital future worthy of our highest aspirations rests on encryption

Encryption, the simple act of scrambling data so that it cannot be read by third parties, keeps us, our loved ones, and our communities safe by protecting everything from private messages to online-banking details and medical records.

It is the foundation of trust in our digital society, as crucial for personal security as it is for national security.

Despite this, encryption is under unprecedented threat from established democracies, which are inadvertently paving a dangerous path that the world's autocrats are only too eager to follow.

Specifically, policymakers in these countries often present strong encryption as being at odds with effective law enforcement. But this is a false choice.

The reality is that we need legislation that protects people online while also maintaining the security infrastructure that safeguards our data. These goals are not mutually exclusive.

Policymakers continue to claim that creating "backdoors" for law enforcement – exceptional government access to encrypted communications – is necessary to help catch criminals.

But cybersecurity research has consistently demonstrated the impossibility of building a backdoor that only the "good guys" can use. A backdoor is a backdoor.

Client-side scanning

The Salt Typhoon case, in which a Chinese government-supported hacker group gained access to US telecom systems by exploiting backdoors originally created for American law enforcement and intelligence agencies, should have sufficed to show that there is no way to control who exploits engineering vulnerabilities built into a system.

However noble their aims, such tools will inevitably become a weapon that criminals, hostile state actors, and malicious hackers can abuse.

Consider the European Union's proposed Child Sexual Abuse Regulation, more commonly known as Chat Control, which would require providers to scan private communications to detect child sexual abuse material (CSAM).

While the goal of protecting children from abuse is urgent and critically important, the proposal would compromise the confidentiality provided by end-to-end encryption.

> Client-side scanning would not stop child sexual abuse material

Under the regulation, providers would have to implement client-side scanning – a technology that scans messages on users' devices before they are encrypted and sent.

If breaking encryption is like ripping open an envelope as a letter passes through the post office, client-side scanning is like having someone reading over your shoulder as you write it.

The result is the same: privacy and confidentiality are lost. Moreover, client-side scanning would not stop CSAM, as perpetrators can circumvent scanning by zipping the photos or copying and pasting them into another file format.

New vulnerabilities

Once such systems are in place, they create new vulnerabilities that hold implications for free speech.

There is no guarantee, for example, that they won't be used to scan for other types of content – political dissent, union organizing, or information that powerful actors want to suppress.

Others, too, face disproportionate harm from weakened encryption. When communications

are compromised, journalists lose the ability to protect sources, hampering efforts to expose corruption.

Medical professionals need encryption to maintain patient confidentiality. Lawyers need it to preserve attorney-client privilege.

Businesses need it to protect trade secrets. Governments need it for national security.

> Breaking end-to-end encryption to "protect children" would, paradoxically, put them at greater risk

For someone escaping domestic violence or living in a community where their identity puts them at risk, encrypted messaging can even be a matter of life and death.

And yes, children need encryption as well. Research from the United Kingdom's Information Commissioner's Office found that encryption strengthens online safety for kids by preventing sexual predators from obtaining sensitive information that could be used for grooming.

Breaking end-to-end encryption to "protect children" would, paradoxically, put them at greater risk.

Public pressure can make a difference

Public pressure can make a difference. The Australian government has not yet compelled tech firms to change their services under its controversial 2018 encryption legislation that gives it the power to issue "technical capability notices," likely because authorities recognize the political risks of using these powers.

In the UK, after civil society mobilized against the Online Safety Act, major companies promised to withdraw their services rather than comply with orders to undermine encryption.

As the Chat Control proposal moves through the EU legislative process, member states are locking horns over encryption

As the Chat Control proposal moves through the EU legislative process, member states are locking horns over encryption.

Poland, the Czech Republic, the Netherlands, and Finland have opposed the legislation in the Council of the EU on the grounds that it threatens privacy, poses national-security concerns, and is ripe for abuse.

But Denmark, France, Hungary, and other countries support it, viewing these risks as worthwhile trade-offs to keep children safe.

The outcome of these political disagreements will be felt far beyond Europe. End-to-end encrypted messaging services are used worldwide, and pressure from a key market like the EU could force firms to compromise the security and privacy of their products, putting users at risk globally.

As the world marks this year's Global Encryption Day, we must recognize that this debate is not about abstract technical specifications.

It is about ensuring that the internet is safe, secure, and trustworthy for all. In terms of protecting children, that means regulations that actually keep them safe, rather than providing false comfort while creating systemic vulnerabilities; targeted law enforcement based on evidence, not mass surveillance; cross-border cooperation to ensure the rapid removal of known CSAM; and robust support for victims and prevention

campaigns.

In other domains as well, we need solutions that address online harms without undermining privacy, confidentiality, and freedom of speech.

A digital future worthy of our highest aspirations rests on encryption. If we want an internet that is for everyone – where people everywhere can connect, communicate, and innovate safely – we must not allow this foundation to erode.

Sally Wentworth is President and CEO of the Internet Society and the Internet Society Foundation.